

UNITED STATES DISTRICT COURT

for the
Eastern District of Tennessee

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

2513 KIRBY AVENUE, CHATTANOOGA, TENNESSEE

Case No. 1:23-mj-

267

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See attachment A, incorporated herein.

located in the Eastern District of Tennessee, there is now concealed (identify the person or describe the property to be seized):

See attachment B, incorporated herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 USC 875

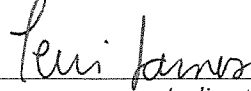
Offense Description
Transmission in interstate commerce of a threat to injure another person

The application is based on these facts:

See affidavit of FBI SA Terrilynn James

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Terrilynn James, FBI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: August 24, 2023

City and state: Chattanooga, TN



Judge's signature

Hon. Christopher H. Steger, US Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TENNESSEE
at CHATTANOOGA

IN THE MATTER OF THE SEARCH OF:
2513 Kirby Ave., Chattanooga, Tennessee

Case No. 1:23-mj-
FILED UNDER SEAL

267

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Terri Lynn M. James, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 2513 Kirby Avenue, Chattanooga, TN 37404 (“the PREMISES”) further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation and have been since November 2007. I have investigated criminal violations involving drug crime, gang criminal enterprises, various financial crimes, terrorism, and wire/mail fraud, among others. I have training and experience in interviewing techniques, arrest procedures, search warrant applications, the execution of searches and seizures, and various other criminal laws and procedures. I am a federal law enforcement officer who is engaged in enforcing criminal laws, including violations of Title 18 of the United States Code.

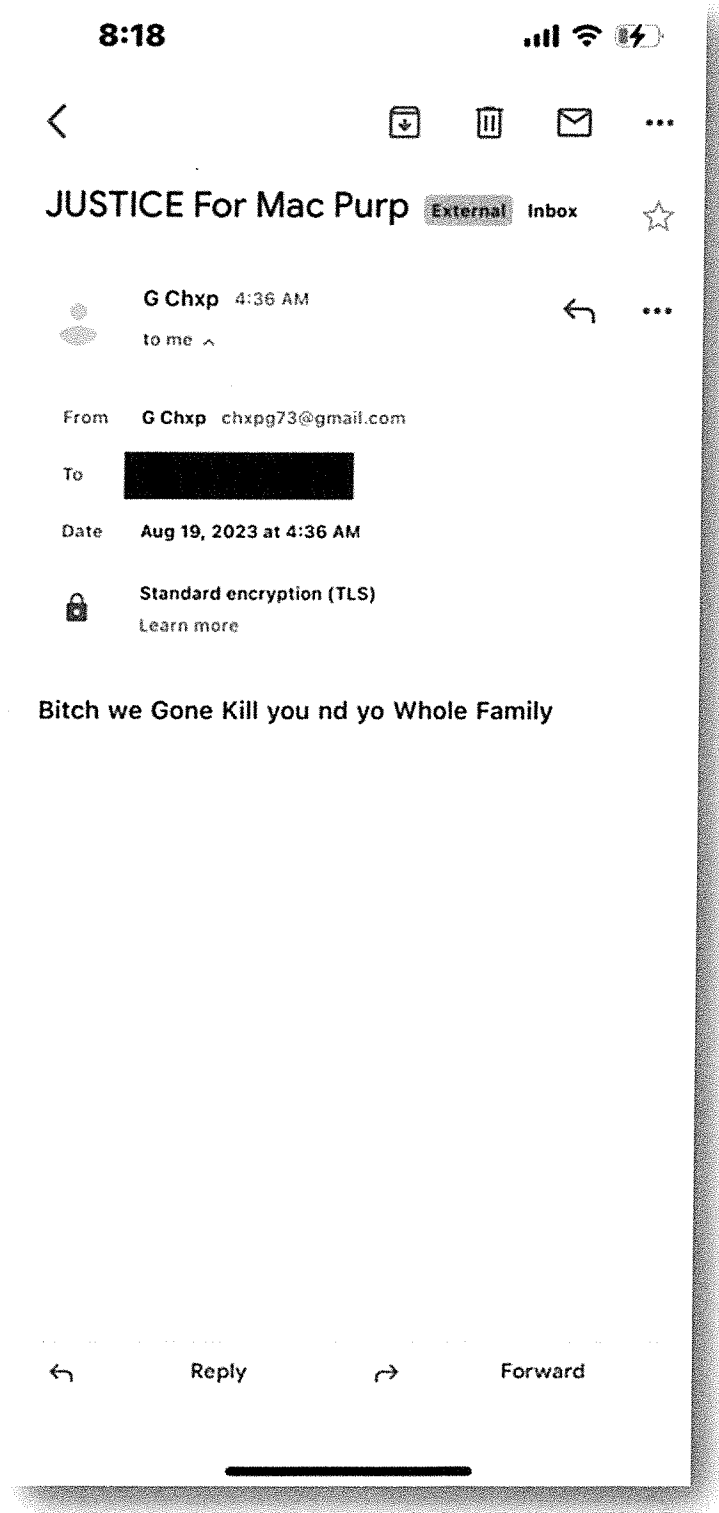
3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §875(c) (i.e. transmission of interstate threats) have been committed, and there is probable cause to search the information described in Attachment A for evidence and/or fruits of these crimes further described in Attachment B

PROBABLE CAUSE

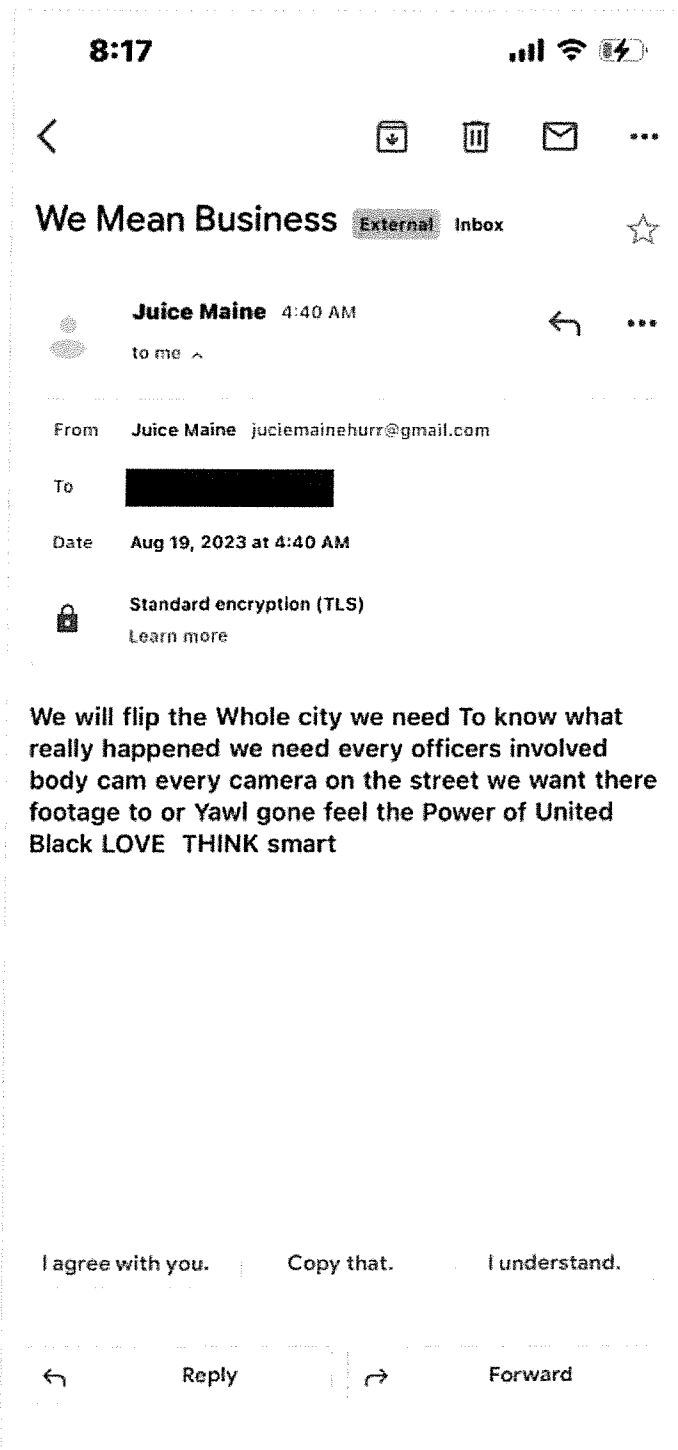
4. On or about August 11, 2023, Chattanooga Police Department (“CPD”) officers were involved in a shooting in Chattanooga, Tennessee, in which Roger Heard, Jr., known by the alias “Mac Purp” exchanged gunfire with police. During the exchange, Mr. Heard and a CPD officer were shot. Mr. Heard died as a result of his wounds. Through open-source and other investigation, CPD personnel learned that certain members of street gangs have authorized or “greenlit” retaliatory violence against law enforcement in the Chattanooga area. Hamilton County officials released video of the incident on August 20, 2023.

5. On August 19, 2023, at 4:36 a.m., the District Attorney General Coty Wamp (of the 11th Judicial District, which includes Chattanooga, Tennessee) received an explicit and threatening e-mail message from an email address chxpg73@gmail.com. The message bore the subject “JUSTICE for Mac Purp.” The message read: “Bitch we Gone Kill you nd yo Whole Family.” A screenshot of the message appears below (with the recipient e-mail address

redacted):



6. At 4:40 a.m., General Wamp received a separate message bearing subject line “We Mean Business” from “Juice Maine” at e-mail address juciemainehurr@gmail.com. A screenshot of the message appears below (with the recipient e-mail address redacted):



7. As a result of these messages, on or about August 19, 2023, law enforcement sent an Emergency Disclosure Request (“EDR”) to Google regarding these e-mail addresses. Results provided in response indicated email account chxpg73@gmail.com is affiliated with a mobile device that was connected to Internet Protocol (“IP”) address assigned to Comcast and that the threatening e-mail appears to have been sent from a residence in Chattanooga.

8. Among other things, email account chxpg73@gmail.com was affiliated with IP address 2601:243:815:38d:c489:3a60:102d:ca69, a Comcast IP address that showed a “last activity timestamp” of August 19, 2023 at 09:46:36 UTC (5:46 a.m. EDT), i.e., approximately one hour after the threatening e-mail was sent. A similar Comcast IP address – bearing the same account information as described in paragraph 12 below – appears to have a “first activity timestamp” dated June 27, 2023, i.e., ten days after the creation of the account, and a “last activity timestamp” of August 19, 2023 at 15:24:03 UTC (11:24 p.m. EDT), i.e., shortly before the EDR was sent. The same Gmail account was affiliated with an IP address belonging to cellular service provider T-Mobile, showing a “last activity timestamp” of August 19, 2023 at 12:18:37 UTC (8:18 a.m. EDT).

9. The disclosure also revealed that email account chxpg73@gmail.com is specifically affiliated with an Android device bearing Android device ID 3f2d3629fd9c113d. That same Android device ID was affiliated with other Gmail accounts, including: juciemainehurr@gmail.com (i.e., the e-mail address from which the second e-mail excerpted

above was sent); shootfirstgetmoneygang@gmail.com; chxpg73@gmail.com; and gbxby704@gmail.com

10. An EDR to Google regarding juciemainehurr@gmail.com showed that it, too, was affiliated with IP address 2601:243:815:38d:c489:3a60:102d:ca69. Data provided by Google indicated a “last activity timestamp” from that IP address as to juciemainehurr@gmail.com of August 19, 2023 at 09:46:36 UTC (5:46 a.m. EDT), i.e., approximately one hour after the threatening e-mail was sent, and the same time as the last activity timestamp provided in response to the EDR concerning chxpg73@gmail.com.

11. A subsequent EDR to Google concerning Android device ID 3f2d3629fd9c113d indicated that the device is a Motorola brand phone, serial number maui:ZY22GXMBRW, IMEI 359687212257357.¹

12. Law enforcement submitted an EDR to Comcast regarding the IP address provided by Google. A representative from Comcast contacted FBI personnel and advised that

¹ In various returns, the Android device ID 3f2d3629fd9c113d is alternatively referred to as an “Android device ID” and an “Android ID.” A subsequent series of EDRs to Google showed this Android device ID affiliated with a separate Android ID (i.e., 4552354352317862205) and a “Google Account” identifier. In any event, the second Android ID (i.e., 4552354352317862205) is assigned to the same IMEI (i.e., 359687212257357), serial number (i.e., maui:ZY22GXMBRW), and “users” (i.e., shootfirstgetmoneygang@gmail.com, juciemainehurr@gmail.com, chxpg73@gmail.com, and gbxby704@gmail.com) associated with both the device and e-mail accounts identified herein.

the IP address was assigned to an account bearing the name “Nina Long” and the address 2513 Kirby Avenue in Chattanooga, Tennessee (i.e., the PREMISES). Comcast further advised that the telephone number assigned to this account is 423-777-0482.

13. Law enforcement was unable to locate anyone at the PREMISES named Nina Long. The property appears to be owned by a property rental/management company located in Hixson, Tennessee.

14. However, a search of law enforcement and open-source data shows that phone number 423-777-0482 is assigned to Kosha Cosey, residing at the PREMISES.

15. An open-source search shows that possible residents of 2513 Kirby Avenue in Chattanooga, TN are Kosha Cosey and Kashawn Cosey. FBI personnel briefly surveilled the residence on August 20, 2023. During that surveillance, law enforcement saw a blue Chrysler parked next to the PREMISES. That car bore Tennessee tag BDF9724, which is registered to Kashawn Cosey at the PREMISES.

TECHNICAL TERMS

16. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IPv4 address traditionally

looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). An IPv6 uses a 128-bit address to greatly expand available addresses, with groups of digits separated by colons (e.g., 2345:0425:2CA1:0000:0000:0567:5673:23b5). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

17. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information – including tablets and mobile devices – all under Rule 41(e)(2)(B).

18. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

19. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how

computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the

United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial

evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. Based on my knowledge, training, and experience, I know that individual users who use multiple devices may cause their separate devices to "cross pollinate," and this occurs intentionally and unintentionally. That is, for instance, certain cloud-storage and other online services offer auto-sync actions that may occur without the user's knowledge, which distributes remnants of information about

the user's activities to various devices on which they are logged in. Digital "cross pollination" can leave important evidence of a user's activity among all of the user's devices and a search that reveals evidence on one device will likely reveal at least remnants of that same information on all of the devices possessed by the same user simultaneously.

20. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic

electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

21. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the

warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

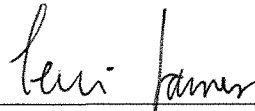
CONCLUSION

22. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

REQUEST FOR SEALING

23. It is respectfully requested that this Court issue an order sealing all papers submitted in support of this application, including the application and search warrant, for a period of 180 days. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,



Terri Lynn M. James
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on August 24, 2023.



Hon. Christopher H. Steger,
UNITED STATES MAGISTRATE JUDGE

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TENNESSEE
at Chattanooga

IN THE MATTER OF THE SEARCH OF:
2513 Kirby Ave., Chattanooga, Tennessee

Case No. 1:23-mj-**267**
FILED UNDER SEAL

ATTACHMENT A

Property to be searched

The property to be searched is 2513 Kirby Avenue, Chattanooga, TN, further described as a beige one-story single-family house, with a white awning over a porch leading to a front entrance. It is marked “2513” on the post attached to the hand railing of the porch.



IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TENNESSEE
at Chattanooga

IN THE MATTER OF THE SEARCH OF:
2513 Kirby Ave., Chattanooga, Tennessee

Case No. 1:23-mj-**267**
FILED UNDER SEAL

ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C § 875(c), those violations occurring after August 18, 2023, until and including August 20, 2023, including:
 - a. Records and information relating to the e-mail account chxpg73@gmail.com;
 - b. Records and information relating to the e-mail account juciemainehurr@gmail.com;
 - c. Records and information relating to threats to law enforcement, including District Attorney General Coty Wamp;
 - d. Records and information relating to the identity or location of the individuals who sent threatening communications to District Attorney General Coty Wamp between August 18 and August 20, 2023;
 - e. Records and information relating to threatening communications sent between August 18 and August 20, 2023, by devices affiliated with Internet Protocol addresses 2601:243:815:14c7:c489:3a60:102d:ca69,

2607:fb90:d71d:b89:94aa:6349:e5a3:43a5,

2607:fb90:3fdb:80d3:751c:bf72:eeca:dda3,

172.56.64.241,

2601:243:815:38d:c489:3a60:102d:ca69, or

2607:fb90:d70a:db09:5c5f:6d6e:f85f:81e9

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks, mobile devices, tablets, or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted

by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.